

METHOD AND SYSTEM FOR HANDLING TWO CA SYSTEMS IN A SAME RECEIVER

Publication date: 2003-03-25

Applicant(s):

- international

- international: H04L9/32; H04N5/00; H04N7/16; H04N7/173; H04L9/32;
H04N5/00; H04N7/16; H04N7/173; (IPC1-7): H04L9/32;
H04N7/173

Application number: JP20010529207T 20001006

Application number: JP20010529207T 20001006

Priority number(s): US19990157968P 19991006; WO2000US27685 20001006

Also published as:

WO0126372 (A1)

MXPA02003524 (A)

ES2225240 (T3)

EP1226717 (A1)

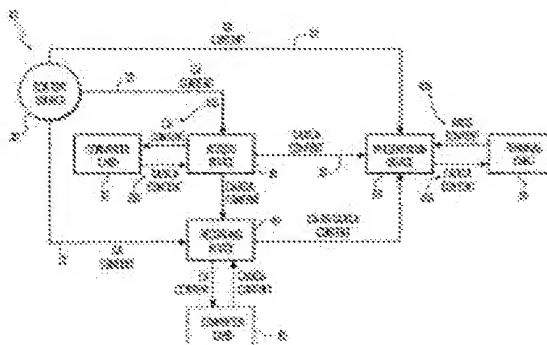
EP1226717 (B1)

[more >>](#)

Abstract of corresponding document: WO 0126372 (A1)

Abstract of corresponding document: WO 0126372 (A1)

A method for enabling a security device to enable an audio/video processing system to permit access to a service, by correctly identifying the service and entitlement message packet. The audio/video transmission systems use multiple conditional access identifications.



Data supplied from the *espacenet* database — Worldwide

(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号
特表2003-511917
(P2003-511917A)

(43)公表日 平成15年3月25日(2003.3.25)

(51)Int.Cl. ⁷	識別記号	F I	キーワード [*] (参考)
H 0 4 N 7/173	6 3 0	H 0 4 N 7/173	6 3 0 5 C 0 6 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 Z 5 J 1 0 4

審査請求 未請求 予備審査請求 有 (全 36 頁)

(21)出願番号 特願2001-529207(P2001-529207)
(86) (22)出願日 平成12年10月6日(2000.10.6)
(85)翻訳文提出日 平成14年4月8日(2002.4.8)
(86)国際出願番号 PCT/US00/27685
(87)国際公開番号 WO01/026372
(87)国際公開日 平成13年4月12日(2001.4.12)
(31)優先権主張番号 60/157,968
(32)優先日 平成11年10月6日(1999.10.6)
(33)優先権主張国 米国(US)

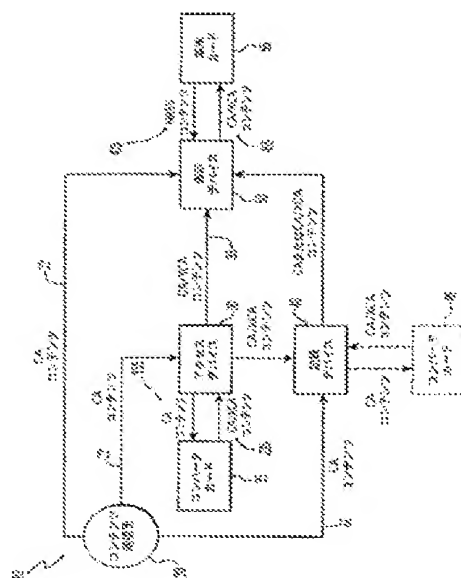
(71)出願人 トムソン ライセンシング ソシエテ ア
ノニム
Thomson Licensing
S. A.
フランス国, エフ-92100 プローニュ
ビヤンクール, ケ アルフォンス ル
ガロ, 46番地
(72)発明者 アーメット ムルジット エスキシオグル
アメリカ合衆国 46250 インディアナ州
インディアナポリス ナンバー125 レ
イクショア トレイル 8235
(74)代理人 弁理士 谷 義一 (外2名)

最終頁に続く

(54)【発明の名称】 同じ受信機において2つのCAシステムを扱うための方法およびシステム

(57)【要約】

サービスおよび資格メッセージパケットを正確に識別することによって、オーディオ/ビデオ処理システムがサービスへのアクセスを許可できるようにすることをセキュリティデバイスに可能にするための方法。オーディオ/ビデオ伝送システムは、複数の条件付きアクセス識別を使用する。



【特許請求の範囲】

【請求項1】 オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、所定の規定に従って前記抽出された対のうちの1つを自動的に識別すること

を含むことを特徴とする方法。

【請求項2】 所定の規定が、前記セキュリティデバイスに前記対が送信される順番によって異なることを特徴とする請求項1に記載の方法。

【請求項3】 前記受信した対のそれぞれが、関連付けられた条件付きアクセス（CA）システムか、拡張条件付きアクセス（XCA）システムのどちらかであることを特徴とする請求項1に記載の方法。

【請求項4】 オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、

サービスおよび資格制御メッセージパケット識別子の対が1つだけ抽出された場合、前記抽出された対を識別し、

サービスおよび資格制御メッセージパケット識別子の複数の対が抽出された場合、所定の規定に従って前記抽出された対のうちの少なくとも1対を自動的に識別すること

を含むことを特徴とする方法。

【請求項5】 所定の規定が、前記対が抽出された順番によって異なることを特徴とする請求項4に記載の方法。

【請求項6】 前記受信した対のそれぞれが、条件付きアクセス資格制御メッセージ識別子か、ローカル資格制御メッセージ識別子のどちらかを含むことを特徴とする請求項5に記載の方法。

【請求項7】 前記受信した対のそれぞれが、サービス識別子をさらに含むことを特徴とする請求項6に記載の方法。

【請求項8】 前記所定の規定が、受信されるべき対の第1の対をサービス識別子およびローカル資格制御メッセージ識別子を含むと定義することを特徴とする請求項6に記載の方法。

【請求項9】 前記データの少なくとも一部が、複数の条件付きアクセスシステムのうちの1つを用いてセキュリティ保護されることを特徴とする請求項4に記載の方法。

【請求項10】 前記条件付きアクセスシステムのうちの少なくとも1つが、前記プログラムの放送業者に関連付けられており、少なくとも第2の条件付きアクセスシステムがアクセスデバイスに関連付けられており、前記表示デバイスと通信可能であることを特徴とする請求項9に記載の方法。

【請求項11】 前記表示デバイスがデジタルテレビジョンであり、前記アクセスデバイスが第2のセキュリティデバイスと組み合わされたセットトップボックスであることを特徴とする請求項10に記載の方法。

【請求項12】 セキュリティデバイスが、インターフェース保護関連情報と条件付きアクセス関連情報とをオーディオ／ビデオ処理デバイスに伝達すること、および

オーディオ／ビデオ処理デバイスが、前記伝達された条件付きアクセス情報と記憶されている条件付きアクセス情報とを用いてプログラムマップテーブルを分解することを含み、

前記プログラムマップテーブルがパケット識別子を対応するサービス情報に関連付けることを特徴とする請求項4に記載の方法。

【請求項13】 前記プログラムを示すデータをデスクランブルするのに適した資格制御メッセージデータをどのパケットが含んでいるかを識別するために、前記セキュリティデバイスが、パケット識別子を使用することを特徴とする請求項12に記載の方法。

【請求項14】 前記資格制御メッセージの少なくともいくつかは、少なくとも、識別およびL E C M用フィールドと、条件付きアクセス識別用フィールドとを含むローカル資格制御メッセージであり、前記正当な処理が、前記識別およびL E C M用フィールドと前記条件付きアクセス識別用フィールドのうちの少な

くとも1つに含まれる情報を用いて前記データの適切な鍵にアクセスすることによって前記サービスをデスクランブルすることを含むことを特徴とする請求項13に記載の方法。

【請求項15】 前記データの少なくとも1つの部分が少なくとも1つのプログラムを示すことを特徴とする請求項9に記載の方法。

【請求項16】 前記データがデジタル伝送システムを介して伝達されることを特徴とする請求項4に記載の方法。

【発明の詳細な説明】**【0001】****(発明の分野)**

本発明は、一般に、デジタルオーディオ／ビデオ伝送システムに関し、より詳細には、デジタルオーディオ／ビデオ伝送システム内の受信機に複数の条件付きアクセス識別を使用することを可能にする方法およびシステムに関する。

【0002】**(発明の背景)**

I S O / I E C 13818-1は、オーディオおよびビデオの1つまたは複数の基本ストリームならびに他のデータの、記憶および伝送に適した単一または複数のストリームへのコーディングを規定する国際規格である。プログラムストリーム(P S)コーディングとトランスポートストリーム(T S)コーディングの2つの形式のコーディングが推奨される。コーディングのプロセスでは、パケット化エレメンタリストリーム(P E S)を獲得するために、まずオーディオビジュアル(A/V)ストリームが圧縮されてパケット化される。P Sは、1つまたは複数のストリームのP E Sパケットを共通の時間基準で結合して単一ストリームにする。T Sは、1つまたは複数のプログラムを1つまたは複数の個別の時間基準で結合して単一ストリームにする。P Sパケットは様々な長さであってよいが、T Sパケットは188バイトの長さである。各T Sパケットは、パケット内に含まれるデータのタイプを識別するパケットID(P I D)を伴う4バイトのヘッダーを有する。P E Sパケットに加え、T Sは、多重分離するためのプログラム仕様情報(P S I)テーブルと現在のプログラムから構成される。プログラムマップテーブル(P M T)は、プログラム番号とそれらを含んでいるエレメントとの間でマッピングを実現するテーブルである。これは、各プログラムに関連付けられたP I Dのリストを含む。

【0003】

アドバンスドテレビジョンシステム委員会(A T S C)は、地上波放送のためのその条件付きアクセス(C A)システムのためにサイマルクリプトアーキテクチャを既に採用している。このアーキテクチャでは、各サービスは、複数の異なる

る独自開発システムに対して、資格管理メッセージ (Entitlement Management Message: EMM) と資格制御メッセージ (Entitlement Control Message: ECM) と共に送信される。この方法で、異なるCAシステムを使用するデコーダは、様々な資格メッセージを信号で伝えるための共通フレームワークを用いてサービスを復号することができる。各サービスは、オーディオパケットとビデオパケットで構成されている。どのデコーダも、それが必要とするパケットを選定し、ストリーム内の他のパケットを無視する。

【0004】

サイマルクリプトベースのCAシステムでは、デジタルテレビジョン (DTV) 等のデジタルオーディオ／ビデオ処理システムは、PMTを分解し、CAモジュールから獲得したCAシステム識別 (ID) を用いてサービスおよびECM PIDを抽出する。通常、各CAモジュールは、1つのCAシステムだけをサポートし、したがって1つのCAシステムIDだけを有する。A/VパケットのPIDと制御ワード (CW) を伝えるECMのPIDとが、正規の購入資格を有するプログラムをデスクランブルするCAモジュールに送信される。

【0005】

(発明の概要)

本発明は、オーディオ／ビデオ処理デバイスがPMTを分解するために2つのCAシステムIDを使用することを可能にし、CAモジュールが特定CAシステムに属するECM PIDを正確に識別することを可能にする。本発明は、A/V処理デバイス例えばDTVが、セキュリティデバイスに、サービスおよび資格制御メッセージ用パケットを正確に識別することによってプログラムにアクセスすることを可能にする方法を含む。このセキュリティデバイスはA/V処理デバイスに関連付けられており、このA/V処理デバイスは、サービスに関連付けられたデータのためにデジタル送信システムに関連付けられている。この方法は、データからサービスおよび資格メッセージ制御パケット識別子の対を少なくとも1つ抽出すること、サービスおよび資格制御メッセージパケット識別子の対が1つだけ抽出された場合、その抽出された対を識別すること、および、サービスお

よび資格制御メッセージパケット識別子の複数の対が抽出された場合、所定の規則に従ってその抽出された対のうちの1つを自動的に選択することを含む。

【0006】

(発明の詳細な説明)

図1は、放送源から、すなわちコンテンツ送信元20を介してコンテンツを受信し、XCAおよびNRSSコピー防止システム（後述）による保護を提供するネットワーク10を示す。コンテンツ送信元20は、例えばテープ、DVD、ケーブル、衛星放送、地上波放送のいずれによっても、経済的価格のあるCAコンテンツ22を提供することができる。コンテンツ22は、通常、保護されており、私設CAネットワークの加入者に供給されるA/Vコンテンツを含んでいる。購入した加入者、またはコンテンツ22を受信する資格を有する加入者には、コンテンツ22をデスクランブルするための必須の鍵が供給される。図1の実施形態によれば、コンテンツ送信元20は、このCAコンテンツ22をアクセスデバイス30、記録デバイス40または表示デバイス50に提供することができる。

【0007】

アクセスデバイス30は、セットトップボックスの形態をとることができる。セットトップボックス30は、XCA/NRSSコンバータカード35と共に動作して、CAコンテンツ22からXCA保護されたコンテンツを作成するが、それはCA/XCAコンテンツ33の一部になる。記録デバイス40は、デジタルVHS（DVHS）またはDVDレコーダの形態をとることができる。記録デバイスは、コンバータカード35に類似したコンバータカード45に提供されても提供されなくてもよい。表示デバイス50は、DVDの形態をとり、CA/XCA保護されたコンテンツをデスクランブルするためにXCA/NRSS端末カード55と共に動作することができる。

【0008】

拡張条件付きアクセス（Extended Conditional Access：XCA）は、コンテンツの配信および販売用の既成および新規のモデルをサポートしながら、伝送および記憶中にMP EG 2符号化デジタルA/Vコンテンツを保護するためのシステムである。XCAは、「再生」および「記録」と

いう基本的な制御を表示制御にマッピングすることによってこのタスクを達成する。XCAシステムにおいて、経済的価値のあるコンテンツは常にスクランブルされている。すなわち、これらのコンテンツは配信者の制御および責任下にあるか、または消費者の家庭、例えばローカル、ネットワークの範囲内にあるものである。XCAはスクランブルされたコンテンツの記録を可能にするが、但しそれは合法的なコピーだけをデスクランブルし、表示することができるということである。非合法的なコンテンツは、デスクランブルされないもので、表示することはできない。非合法的なコンテンツとは、例えば原作でないものや著作権所有者の承認を受けていないもののことである。

【0009】

XCAは3段階の資格を提供する。無制限に自由に配信されるコンテンツは、「コピー自由」コンテンツである。このコンテンツの例としては、広告が流され、提供を受けている放送テレビジョン、インフォマーシャル、または類似の素材を挙げることができる。「1回コピー済み(c o p y - o n c e)」またはローカル表示プログラミングコンテンツは、単一の家庭またはローカルネットワーク内で作成され、何回でも表示することができる。しかしながら、このようなコピーは他のローカルネットワークに転送することができない。このタイプのコンテンツの例としては、スポーツイベントまたは割増金サービスを挙げることができる。最後に「コピー不可」または即時表示プログラミングコンテンツは、リアルタイム表示だけを可能にし、すなわち記録されたコピーは表示不可能である。このタイプのコンテンツの例としては、従量料金制プログラミングまたは他的高額コンテンツを挙げることができる。

【0010】

XCAアーキテクチャに特徴的な特性は、条件付きアクセスとローカルプロテクションの概念である。ローカルプロテクションまたはセキュリティは、アクセスデバイス、例えば30が、スクランブルされたプログラム、例えばCAコンテンツ22を受信した後における、ホームネットワークの範囲内におけるコンテンツの保護である。これは、表示デバイス、例えば50が、何に対してアクセス権を有しており、したがって、保護されているどのコンテンツを変換し、表示する

ことができるかを規定している。取り外し可能なセキュリティデバイス、例えばコンバータカードおよび端末カード35、45、55は、セキュリティ関連の機能を実施する。経済的価値のあるコンテンツはCAサービスを使用して配信される。例えばデジタル衛星システムは、そのシステムの加入者に対する大量配信用ビデオコンテンツおよび鍵をスクランブルする。一部の加入者はそのコンテンツの購入を決定することができるが、その場合、その加入者にはそのコンテンツをデスクランブルして表示するために必須の鍵が供給される。コンテンツを購入しないことを選択した加入者には、これらの鍵へのアクセス権は提供されない。XCAでは、デスクランブルするための鍵は、一意のローカル公開鍵によって保護される新しいECMに再バンドルされる。ローカルECM（LEMC）を使用してコンテンツを受信する表示デバイスは、したがって特定のCAシステムによって保護されるコンテンツだけを処理するのではなく、同様にXCAによって保護されるコンテンツを処理することも必要となる。

【0011】

次に図2を参照すると、システム10における使用に適した汎用XCA家庭用電化製品（CE）デバイス60が示されている。特定のタイプのデバイス60は特有の機能を有している。例えばXCAアクセスデバイス30はCA/XCA33に対するXCA保護されたコンテンツを作成し、XCA表示デバイス50はXCA保護されたコンテンツをデスクランブルし、XCA記録デバイス40は、コンバータカード45が提供されていない限り、XCA保護されたコンテンツを記憶し、再生はするが、これを作成したりデスクランブルすることはできない。一般に、汎用デバイス60には、切替ユニット（switching unit）62、入力ユニット61、および更新可能なまたは組込み型のセキュリティデバイス66、例えばコンバータカード35または45、または端末カード55が含まれる。そのデバイスのタイプによって、デバイス60には、表示ユニット64、記憶ユニット68、アナログ出力65、圧縮解除されたデジタル出力67または圧縮されたデジタル出力69も含まれる場合がある。

【0012】

デジタル入力ユニット61は、一般に、例えば復調器等の、デジタル信号を獲

得するために必要な回路およびソフトウェアを含む。圧縮されたデジタル出力69は、例えば変調器等の、MPEG2デジタル信号を発行するための回路およびソフトウェアを使用する。セキュリティデバイス66は、CA機能とXCA機能とを操作してコンテンツのタイプを変換することができる。これは、変換されたコンテンツをデジタル形式で出力するモデルの唯一の素子である。前述の通り、セキュリティデバイス66は、コンバータカード35または45、または端末カード55の形式をとることができる。コンバータカード35および45は、(1) CA資格を検査すること、(11) 制御ワード(CW)回復、(111) コンテンツのデスクランブル等の機能をサポートする。これは、三重データ暗号化規格(TDES)鍵を生成し、そのコンテンツを再スクランブルし、その公開鍵を使用してLECMを暗号化する。端末カード55は、XCA資格を検査すること等の機能をサポートする。これは、LECMのCWを用いてコンテンツをデスクランブルし、次いでXCA NRSSインターフェース保護システムの要件に従ってそのコンテンツを再スクランブルする。例示的コンバータカード35と端末カード55のブロック図を、それぞれ図3および図4に示す。記憶ユニット68は、不揮発性メモリにコンテンツを記憶し、そこからコンテンツを読み出す。記憶ユニット68は、コンバータカード45が提供されていない限りコンテンツのタイプを変換せず、その場合、記憶ユニット68はアクセスデバイスとしても動作する。ハードディスクは典型的な内部記憶ユニットである。デジタル揮発性ディスク(DVD)プレーヤおよびDVHS等のデジタルビデオテープレコーダは、典型的な取り外し可能記憶装置付きCEデバイスである。表示ユニット64は、MPEG2コンテンツを復号し、それをユーザにアナログ形式または圧縮解除されたデジタル形式で提示する。表示ユニットは、NRSSデスクランブラー64'を用いてNRSSストリームをデスクランブルすることができ、MPEGデコーダ64''を用いてデジタルストリームを復号することができ、デジタルアナログコンバータ(DAC)64'''を用いてデジタルアナログ変換を実施することができる。最終結果は、音声またはアナログ電子信号等の物理信号である場合がある。ハイファイ増幅器のTVディスプレイおよびアナログ出力は典型的な例である。切替ユニット62は、デバイス60内でコンテンツを経路指定する。

その機能は経路指定のみに限定され、コンテンツのタイプは変更しない。

【0013】

XCAシステムは、XCA端末カード55を表示デバイス50に接続するNRSSインターフェースを保護するように設計されている。コンテンツがCA/XCAコンテンツなので、NRSSインターフェース保護はアクセスデバイス30では必要とされない。

【0014】

XCA保護されたNRSSインターフェースを設定する手順では、表示ホストデバイス50を認証すること、特定の表示デバイス50/端末カード55の対に対して一意の共用秘密鍵を設定すること、コンテンツ保護用共用鍵を作成すること、データ暗号化規格(DES)および共用鍵によってホスト50に戻るコンテンツをスクランブルすること。

【0015】

ローカル資格制御メッセージ(LECM)は、表1のシンタックスによって長さが可変であることができる1つまたは複数のセクションに含めることができる。セクションの始めは、パケットペイロードのポインタフィールドで示すことができる。

【0016】

【表1】

表 1

シンタックス	ビット数	ニーモニック
Local_Entitlement)Control_Message{		
Table_id	8	0×80 または 0×81
Section_syntax_indicator	1	'1'
Private_indicator	1	'1'
Zero	2	'00'
Private_section_length	12	Uimbsbf
Table_id_extension(){		
Reserved	6	'000000'
LECM_type	2	'10'
Protocol_version	8	Uimbsbf
}		
Reserved	2	'11'
Version_number	5	'00000'
Current_next_indicator	1	'1'
Section_number	8	0×00
Last_section_number	8	0×00
XCA_identifier	256	Uimbsbf
Local_source_id	64	Uimbsbf
Reserved	5	Uimbsbf
Copy_protect_enable	1	Uimbsbf
XCA_view_flag	2	Uimbsbf
Time_code	32	Uimbsbf
Source_sequence_number	32	Uimbsbf
XCA_descriptor	424	Uimbsbf
Padding_bytes	508	Uimbsbf
Integrity_check	32	Uimbsbf
CRC_32	32	Rpchof

【0017】

ここで、

Table_id この8ビットフィールドは、このセクションが属している資格制御メッセージを識別する。0×80または0×81のどちらかにセットされる。LECMセクションにおいて少なくとも1ビットの変更がある場合、このtable_idは切り替わる。

【0018】

`Section__syntax__indicator` この1ビットのフィールドは「1」にセットされる。これは、そのセクションが、セクション長さフィールドを超えて汎用セクション構文に続くことを示している。

【0019】

`Private__indicator` この1ビットのフィールドは「1」にセットされる。

【0020】

`Private__section__length` この12ビットのフィールドは、`private__section__length`フィールド直後から続けて始まり、CRC__32を含めて、このセクション内の残りのバイト数を明記する。

【0021】

`LECM__type` この2ビットのフィールドは、LECMによって伝えられる情報のタイプを示す。「10」は、これが制御ワードを伝えていることを意味している。

【0022】

`Protocol__version` 8ビットの符号のない整数フィールドであって、その機能は、現行プロトコルにおいて定義されているパラメータと異なって構造化し得るパラメータを、将来、この表が伝えることを可能にするものである。現在はプロトコルが1つだけ定義されている。`Protocol__version=0x00`の場合、プログラム全体に対して単一の制御ワードの対が使用され、同様に、プログラム全体に対してアクセス基準が規定される（すなわち、ストリームレベルの保護は許可されない）。この場合、その事象のすべてのストリームは同じ制御ワードによってスクランブルされ、同じアクセス基準を使用する。`Protocol__version=>0, 01`の場合、`0x00`よりも大きな`protocol__version`の値は、そのプロトコルの将来のバージョンが導入された際にそのバージョンに合わせて設計されたデコーダによって処理されることだけが可能である。

【0023】

`Version__number` この5ビットのフィールドは予約されており、「00000」の値を有する。将来の実施態様は、必要に応じてこのフィールドを使用することができる。

【0024】

`Current__next__indicator` この1ビットのインジケータはLECMのために常に「1」にセットされており、送信されるLECMは常に現行で適用可能である。

【0025】

`Section__number` この8ビットのフィールドは、いくつかのプライベートセクションを含んでいる。プライベートテーブル内の第1のセクションのセクション番号は0×00になる。このセクション番号は、このプライベートテーブルに属する付属セクションごとに1つずつ増分される。

【0026】

`Last__section__number` この8ビットのフィールドは、このセクションをその一部として含むプライベートテーブルの最後のセクション番号を示している。

【0027】

`XCA__identifier` この256ビットのフィールドは一意的なXCA識別子を含んでいる。この識別子は、「著作権：(C) 1999 TMM」というASCII値を有する。引用符は含まれない。各ASCII文字には1バイトの記憶が割り当てられている。このフィールドでは文字は左寄せされる。未割当てのフィールド値は0×00にセットされる。

【0028】

`Local__source__id` この64ビットのフィールドは、このLECMを生成したセキュリティデバイスのXCAデバイスIDを含んでいる。

【0029】

`Copy__protect__enable` この1ビットのフィールドは、表示デバイスから出力されるプログラムマテリアルの1つまたは複数のストリー

ムのためのコンテンツ保護機構があることを示す。このフラッグの目的は、ユーザに対して故障表示を検出するための手段を提供することであり、コピー防止を強制するために使用されるものではない。少なくとも1つのストリームに対する保護が使用可能である場合、このフィールドの値は「1」にセットされる。

【0030】

`XCA__view__flag` この2ビットのフィールドの値は、XCA保護に変換する前にプログラムコンテンツの保護を管理する管理権限によって判定される。この値は、`XCA__descriptor`における`XCA__view__flag`の値と照合される。不一致の場合、XCA表示デバイスのセキュリティプロセッサ内で表示権を行使するために、保護される`XCA__view__flag`が使用される。意味体系は以下の通りである。

【0031】

`XCA__view__flag = '00'` : XCAコンテンツは制限されない。いつでも、どこでも表示してよい。
`XCA__view__flag = '01'` : XCAは予約されている。
`XCA__view__flag = '10'` : XCAコンテンツはローカルネットワーク内ではいつでも表示してよいという制限を受ける。
`XCA__view__flag = '11'` : XCAコンテンツはローカルネットワーク内で「今」だけ表示してよいという制限を受ける。

【0032】

`Time__code` タイムソースが周知でありセキュリティ保護されている場合、このフィールドは、1980年UTC 1月6日午前12時から発生している秒数を含んでいる ($\text{mod } 2^{32}$)。タイムソースが周知でもなくセキュリティ保護もされていない場合、このフィールドはすべて0に符号化される。

【0033】

`Source__sequence__number` この32ビットのフィールドは、LECMを作成したコンバータモジュールの暗号期間カウンタを含んでいる。

【0034】

`Padding__bytes` LECMのセキュリティ保護された部分の合

計の長さ(128-65)を128バイトにするために必要とされるバイト数である。このpadding_byteはランダムに選択される。

【0035】

Integrity check この32ビット数のフィールドは、暗号解除されたペイロードのコンテンツが有効であることを確認する値を含んでいる。これは、暗号化プロセスと暗号解除プロセスとが適切に実施されることを保証するために使用される。

【0036】

CRC-32 この32ビットのフィールドは、LECMセクション全体を処理した後でISO/IEC 13818-1「MPEG2 Systems」付録Aで定義されているデコーダのレジスタからのゼロ出力を保証するためのCRC値を含んでいる。この値は、データが暗号化された後で計算される。

【0037】

各コンバータカード35は、CA保護されたコンテンツからXCA保護されたコンテンツへの変換をサポートし、32ビットの暗号期間カウンタを有する。暗号期間は、ストリームまたはプログラムが1つの特定の鍵によってスクランブルされる期間と定義される。新しい暗号期間ごとに、すなわち、制御ワードが変更する度に、コンバータモジュールはその暗号期間カウンタを1つ増分する。例えばプログラムが異なる暗号期間を有する3つのストリームを含む場合、このカウンタは各ストリームの各暗号期間の開始時点で増分される。外部からのアクセスに対して保護されているので、このカウンタがリセットされたり減らされたりすることは有り得ない。暗号期間の初期値は0である。

【0038】

コンバータカード35は、そのコンテンツへのアクセスが合法であると判定すると、LECMを作成するために次の情報を使用する。すなわち、奇数と偶数のCW、コピー制御情報(CCI)、および、例えば「表示自由」、「ローカル表示のみ」、「現時点での表示のみ」の3つの実現可能な状況のうちの1つであるようなコピー防止(CP)状況である。

【0039】

C A 保護されたコンテンツから X C A 保護されたコンテンツへの変換は次のプロセスを含む。すなわち、コンバータカード 35 がその X C A ____ I D を L o c a l ____ s o u r c e ____ i d に割り当てる。コンバータカード 35 は、コンテンツが「現時点での表示のみ」のタイプである場合は c o p y ____ p r o t e c t ____ e n a b l e を 1 にセットし、そうでない場合は c o p y ____ p r o t e c t ____ e n a b l e は 0 にセットされる。コンバータカード 35 は暗号期間カウンタの現行値を s o u r c e ____ s e q u e n c e ____ n u m b e r に割り当てる。また、コンバータカードは、L E C M のセキュリティ保護された部分で計算されたハッシュ値を i n t e g r i t y ____ c h e c k に割り当てる、というプロセスである。

【0040】

ハッシュ方法は、本発明の一態様によれば以下の通りである。

【0041】

【数1】

$$\begin{aligned} C[0] &= M[0] \oplus M[4] \oplus \dots \oplus M[4 \times (n/4)] \\ C[1] &= M[1] \oplus M[5] \oplus \dots \oplus M[4 \times ((n-1)/4) + 1] \\ C[2] &= M[2] \oplus M[6] \oplus \dots \oplus M[4 \times ((n-2)/4) + 2] \\ C[3] &= M[3] \oplus M[7] \oplus \dots \oplus M[4 \times ((n-3)/4) + 3] \end{aligned}$$

【0042】

上式で、M [i] は、暗号化すべきメッセージの i 番目のバイトを表しており、シーケンスの第 1 のバイトは指標 0 を有しており、C [i] は i n t e g r i t y ____ c h a c k フィールドの i 番目のバイトを表しており、フィールドの第 1 のバイトは指標 0 を有する。

【0043】

L E C M のセキュリティ保護された部分は R S A - 1 0 2 4 を使用して暗号化される。暗号化鍵は、コンテンツが「表示自由」のタイプの場合は自由表示公開鍵である K p u b ____ f r e e であり、そうでない場合、これはコンバータカードの公開鍵である K p u b ____ i である。最後に、コンバータカードは、L E C M のセキュリティ保護された部分を暗号化した後で C R C ____ 3 2 を計算する。

【0044】

再び図3を参照すると、例示的コンバータカード35のブロック図が示されている。コンバータカード35は、CAシステム100と、XCAシステム200とを含む。CAシステム100は、一般に、リンク37を介してホストデバイスと通信するISO—7816リンクデバイス110、例えばアクセスデバイス30と、CA操作可能ソフトウェア(SW)120と、ECMおよびECM抽出器(extractor)130、140と、三重日付暗号化規格(TDES)デバイス150とを含む。TDESデバイス150、およびECMおよびECM抽出器130、140には、ホストからCAコンテンツを受信するための入力155が設けられ、供給されている。TDESデバイス150は出力160をさらに含む。XCAシステム200は、一般に、XCA操作可能ソフトウェア220とECM置換モジュール230とを含む。ECM置換モジュール230は、出力160を介してTDES変換モジュール150と通信することができる。ECM置換モジュール230には、ホストにXCAコンテンツを戻すための出力235がさらに提供されている。

【0045】

端末カード55は、XCA保護されたコンテンツからNRSSコンテンツへの変換をサポートする。この目的のために、端末カード55は、それ自体に連結されているコンバータカード35(i)ごとにその記録を保持する。この記録は以下のフィールドを含んでいる。すなわち、コンバータカード35(i)のXCA__ID、コンバータカード35(i)の秘密鍵Kpriv__i、およびコンバータカード35(i)から受信したsource__sequence__number__SSN_iの最新の値である。XCA保護されたコンテンツからNRSSコンテンツへの変換には、CRC__32の値がLECMから計算された値と一致しない場合、端末カード55がその変換を取り消すことを含む。XCA__view__flagによって定義されるコンテンツの状況が「表示自由」のタイプに相当する場合、暗号解除鍵は自由表示秘密鍵Kpriv__freeである。端末カード55は、RSA—1024を使用してLECMのセキュリティ保護された部分の暗号解除を行う。暗号化されていないlocal__source__idから、端末

カード55は発行しているコンバータカード35を識別する。端末カード55が対応する秘密鍵をまだ有していない場合、すなわち、端末カード55が、その第1のフィールドが`local__source__id`の値に等しい記録を有していない場合、端末カード55はその変換を停止し、秘密鍵の要求を開始する。そうでない場合、端末カード55は、`local__source__id`で識別されるコンバータカード35に関連付けられた秘密鍵を使用して、RSA-1024でLECMのセキュリティ保護された部分を暗号解除する。未暗号化部分の`XCA__view__flag`の値がXCA記述子の`XCA__view__flag`の値と一致しない場合、端末カード55はその変換を取り消す。コンテンツが「現時点での表示のみ」タイプに相当する場合、端末カード55は、2つの検査によって再生がないことを保証する。セキュリティ保護されたタイムソースがホストに対して使用可能でない場合、第1の検査は省略される。第1の検査において、端末カード55は、`time__code`を、NRSSコマンドを用いて表示デバイス50から受信したホストタイムと照合する。その差が所定の量、例えば5分よりも多い場合、端末カード55はSSNiを`source__sequence__number`と照合する。そうでない場合、端末カード55はその変換を取り消す。第2の検査では、SSNiが`source__sequence__number`よりも少ない場合、端末カード55は対応するSSNiを更新し、LECMのCWを用いてコンテンツをデスクランブルする。そうでない場合、端末カード55はその変換を取り消す。コンテンツが「現時点での表示のみ」タイプに相当しない場合、端末カード55はLECMのCWを用いてコンテンツをデスクランブルする。端末カード55は、CCIフィールドのコンテンツをNRSS保護の目的でNRSSモジュール300に渡す。最後に、端末カード55は、NRSSモジュール300にそれぞれの新しい暗号期間の発生を伝達する。

【0046】

別の変換では、XCA保護されたコンテンツはクリアコンテンツに変換される。この変換は、XCA保護されたコンテンツをNRSSコンテンツに変換することに類似しているが、これらの顕著な違いは、例えばクリアコンテンツはデバイス60の切替ユニット62に直接的に渡され、CCIはホストプロセッサに直接

的に渡されるということである。

【0047】

再び図4を参照すると、例示的端末カード50のブロック図が示されている。一般に、端末カード50は、CAシステム400とXCAシステム300とを含む。CAシステム400は、一般に、ホストデバイスと通信可能なISO—7816リンクデバイス410、例えばリンク57を介する表示デバイス50と、CA操作可能ソフトウェア(SW)420と、ECMおよびEMM抽出器430、440と、三重日付暗号化規格(TDES)デスクランブルデバイス450とを含む。ホストからCA/XCAコンテンツを受信するための入力455がTDESデバイス450、ECMおよびEMM抽出器430、440に設けられ、供給されている。TDESデバイス450は、出力460をさらに含んでいる。XCAシステム300は、一般に、XCA操作可能ソフトウェア320、NRSSコピー防止操作可能ソフトウェア(SW)340、およびNRSSコピー防止(CP)モジュール350とを含む。NRSSコピー防止(CP)モジュール350は、出力460を介してTDESデスクランブルモジュール450と通信可能である。NRSSコピー防止(CP)モジュール350には、NRSSコンテンツをホストに戻すための出力435もさらに設けられている。

【0048】

端末カード55は、それ自体のタスクを完了するために、ホストデバイス50とデータを交換する。この通信は、例えばNRSS EIA—679B準拠コマンドを用いて実行することができる。該当するNRSS規格によれば、どの動作を実行する必要があるかを決定するためにホストは定期的にカードの状況を監視する。

【0049】

ナショナルリニューアブルセキュリティスタンダード(NRSS: National Renewable Security Standard)は、継続可能なセキュリティを、DTV受信機およびデジタルVCR等のデジタル家庭電化(CE)デバイスで使用するための手段を提供する。したがってこのセキュリティ機能は、ナビゲーションalデバイス(navigational devi

c e) からは分離されている。端末カード55のようなNRSSセキュリティデバイス、表示デバイス50のようなそのホストデバイスから保護されたコンテンツを受信すると、そのコンテンツをデスクランブルし、それをホストデバイスに返送する。コンテンツはセキュリティデバイスを離れる前はクリアな状態なので、インターフェース全体を通して保護される必要がある。NRSS規格は、また、暗号ベースのコピー防止システムに対するフレームワークを定義する。

【0050】

NRSS規格によれば、ホストと端末カードは、1つまたは複数のNRSSコピー防止システムに対するサポートを有するように製造することができる。これらのシステムは、一意のコピー防止(CP)システムIDによって識別される。どのシステムが実施されるかを判定するために、端末カード55とそのホストデバイス50との間でネゴシエーションを使用することができる。端末カード55の初期化の一部として、ホスト50は、それがサポートするNRSSコピー防止システムに関して端末カード55に報告する。XCA NRSSコピー防止システムがこのセットに含まれている場合、端末カード55は、CAシステムIDをも含むその構成と共にCPシステムIDを返送する。この構成を検討して、ホスト50は、XCAと特定のCAシステムの両方が端末カード55によってサポートされていることを認識し、その後、XCAシステムIDとCAシステムIDの両方を用いてPMTを分解する。新しいプログラムごとに、カード55はホストからサービスとECM PIDを獲得する。本発明の一態様によれば、XCA CAシステムIDは、それがデータの機密部分でないかのようにXCAコピー防止システムをサポートするホストデバイスに記憶されており、セキュリティ保護された記憶装置を必要としない。

【0051】

構造によって、端末カード55は、放送事業者のヘッドエンドおよびホームネットワークにおける再生デバイスを含めて、様々な送信元から入来するCAおよびXCAストリームの両方を処理する。受信したコンテンツに応じて、ホスト、例えば表示デバイス50は端末カード55に{サービスPID、ECM PID}の1つまたは複数の対を返送することができる。ここで、次の3つの可能性が

ある。すなわち(1) 1対だけが送信される、すなわち、LECM PIDを含んでいる {サービスPID、ECM PID} である。(2) 1対だけが送信される、すなわち、CA ECM PIDを含んでいる {サービスPID、ECM PID} である。または(3) 2対が送信される。すなわち、LECMを含んでいる1対と、CA ECM PIDを含んでいるもう1対である。したがって、CA ECMとLECMとを区別する必要がある。2つの例示的ケースを提供する。

【0052】

ケース(a)：2つの対が提供される場合。第1の対 {サービスPID、ECM PID} が、規定により、PIDのうちの所定の1つ、例えばLECM PIDまたはCA ECM PIDと定義される。

【0053】

ケース(b)：1対だけが提供される場合。端末カードが、表1に関して議論したように、LECMをそれらのシンタックスを検査することによって検出する。本発明の別の態様によれば、この目的のために使用することができる2つのフィールドはLECM__typeとXCA__identifierである。前者は転送パケットが伝えるものを示し、後者はXCA LECMに対する一意の識別子を提供する。

【0054】

例えば、(1) ビデオPID：100と、(2) オーディオPID：101のサービスPIDを有するPIDを想定する。これら2つの基本ストリームは同一鍵によって保護される。デスクランブルする鍵は、2つのCAシステムによって保護されるECMで伝えられる(2つのCAシステムより多くのCAシステムがあってもよい)。すなわち、(1) CAシステム#1 ECM PID：180および(2) CAシステム#2 ECM PID：181である。CAシステム#1用のECMはPID182を有するLECMに変換され、置換される。次にホストデバイスは表2によって特徴づけられるように、カードに2つの対(サービスPID、ECM PID)を送信する。

【0055】

【表2】

表 2

サービス P I D	ECMPID
100	182
101	182
100	181
101	181

【0056】

複数対のうちの第1の対が規定によって L E C M P I C にセットされた場合、P I D 1 8 2 は L E C M に対して P I D であると識別される。

【図面の簡単な説明】

【図1】

放送源からコンテンツを受信し、X C A および N R S S コピー防止システムを使用してコピー防止を提供するように構成されているネットワークを示す図である。

【図2】

図1のシステム内で使用されている X C A デバイスのブロック図である。

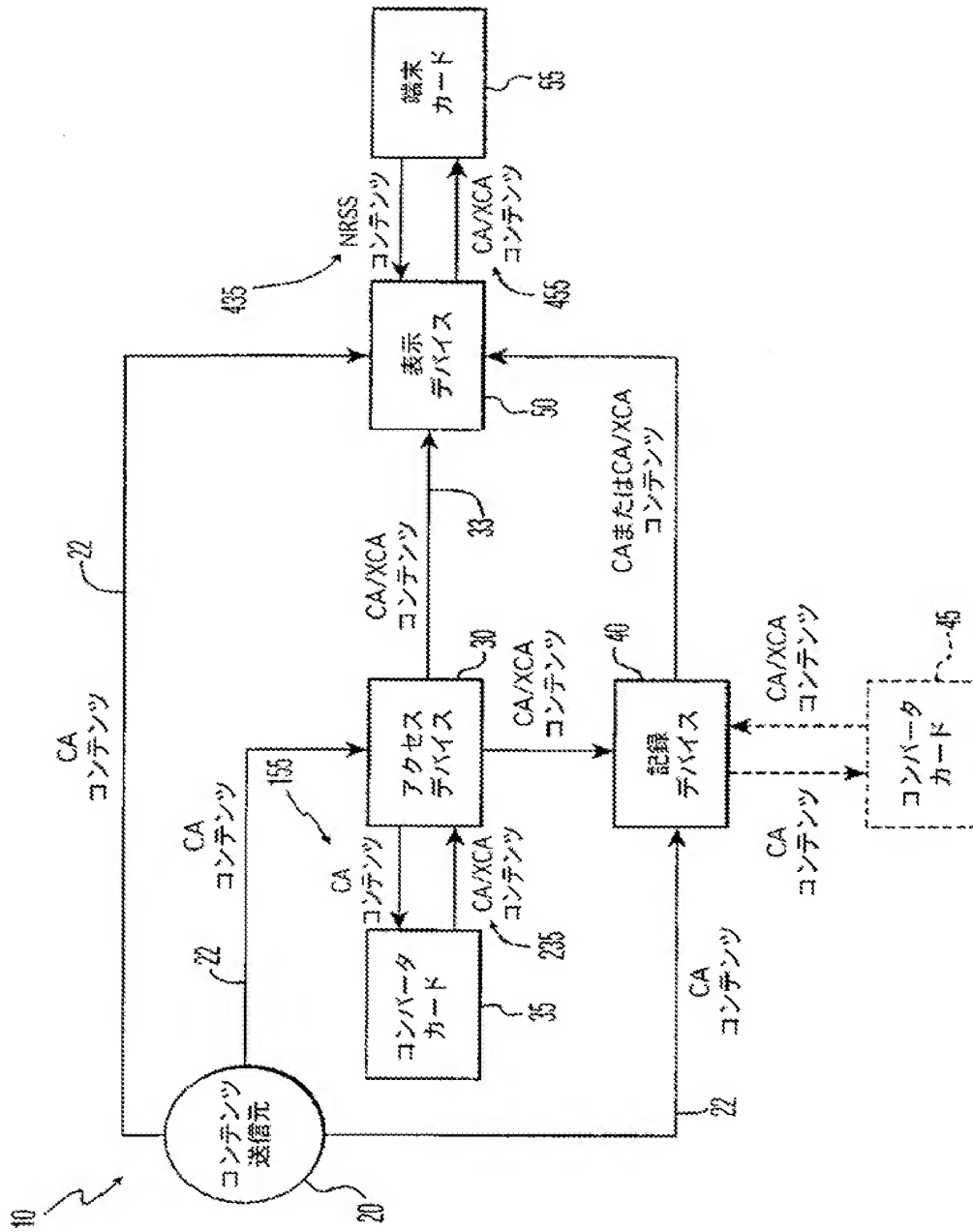
【図3】

本発明の一態様で利用されるコンバータカードのブロック図である。

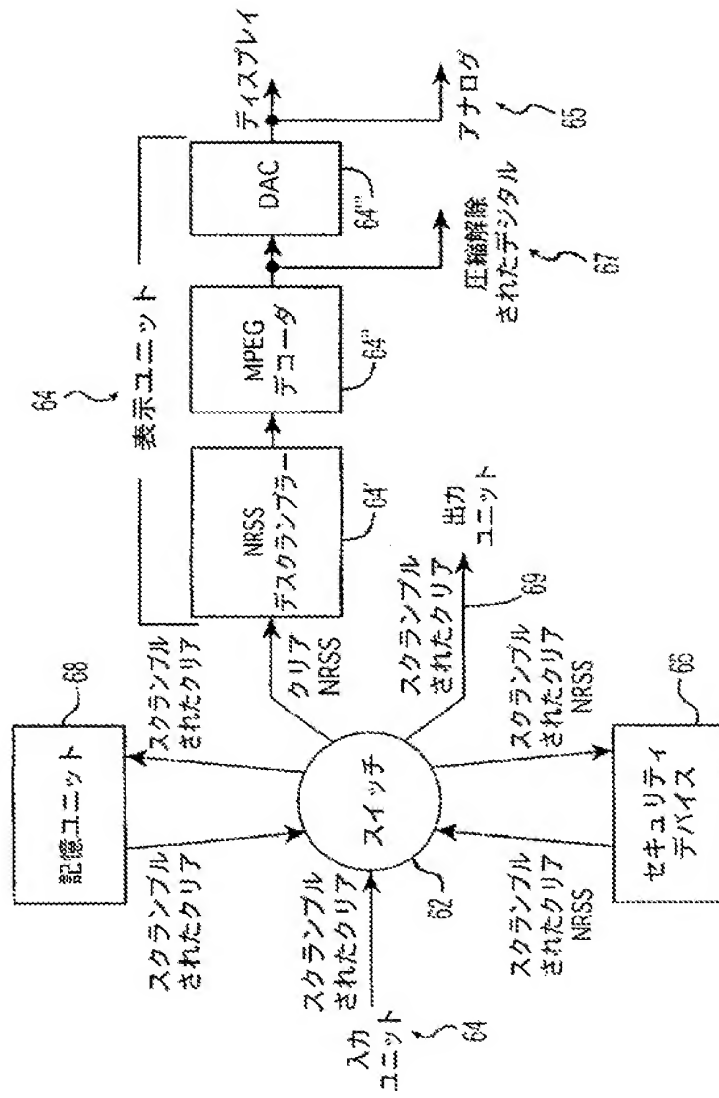
【図4】

本発明の一態様で利用される端末カードのブロック図である。

【図1】



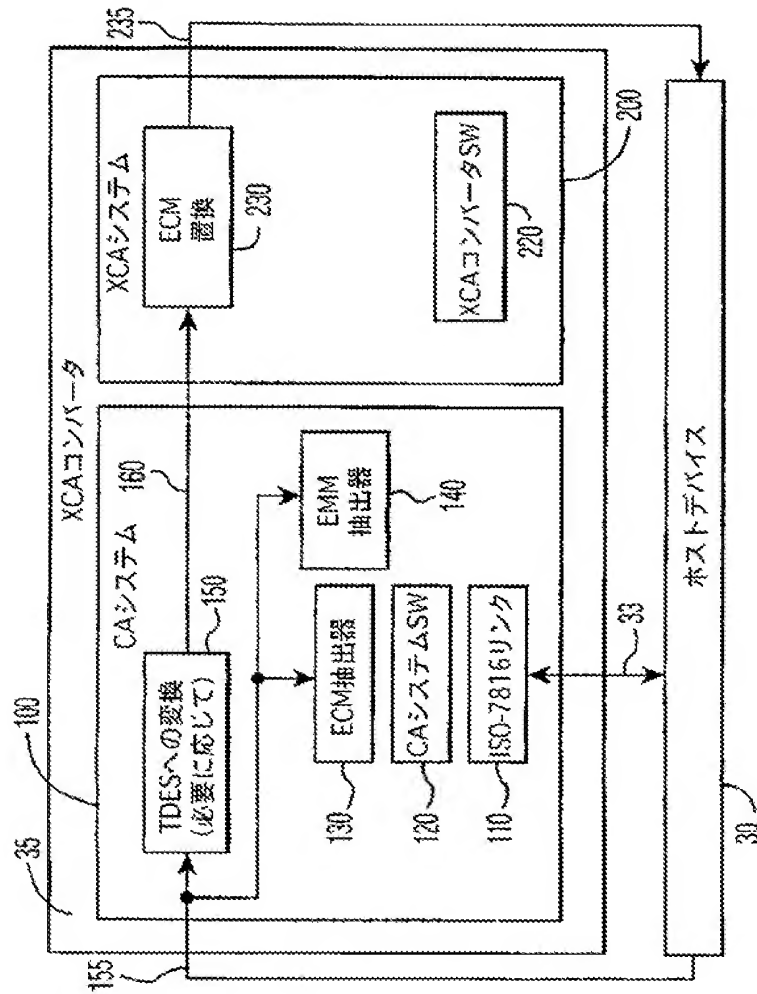
【図2】



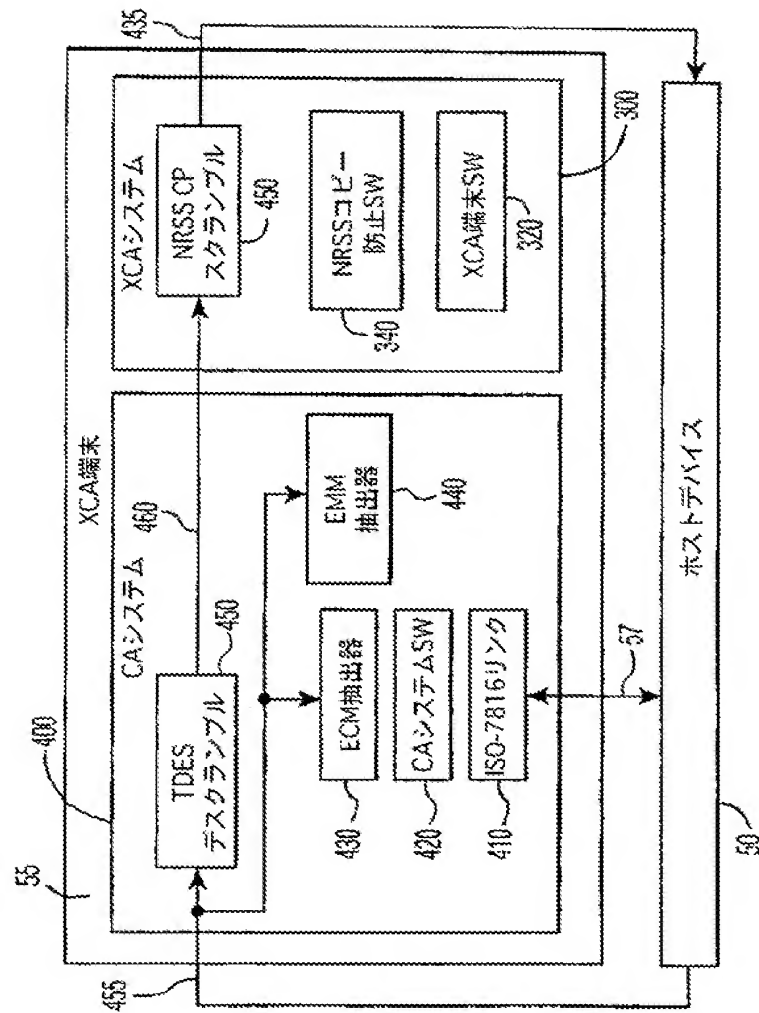
コンテンツのタイプ

スクランブルされたもの：CAおよびXCAコンテンツ。クリアなもの：未スクランブルのMPEG転送ストリーム。
 NRSS：単一DESスクランブルされた転送ストリーム。このコンテンツは、1つまたは複数のデスクランブル
 する鍵が使用不可能の場合、スクランブルされたコンテンツと判別不可能である。

【図3】



【図4】



【手続補正書】特許協力条約第34条補正の翻訳文提出書

【提出日】平成13年10月24日(2001. 10. 24)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】 オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、所定の規定に従って前記抽出された対のうちの1つを自動的に識別することを含み、

前記受信した複数の対のそれぞれが、条件付きアクセス資格制御メッセージ識別子(CA E C M)またはローカル資格制御メッセージ識別子(L E C M)のどちらかを含むことを特徴とする方法。

【請求項2】 所定の規定が、前記セキュリティデバイスに前記対が送信される順番によって異なることを特徴とする請求項1に記載の方法。

【請求項3】 前記受信した対のそれぞれが、関連付けられた条件付きアクセス(CA)システムか、拡張条件付きアクセス(XCA)システムのどちらかであることを特徴とする請求項1に記載の方法。

【請求項4】 オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、

サービスおよび資格制御メッセージパケット識別子の対が1つだけ抽出された場合、前記抽出された対を識別し、

サービスおよび資格制御メッセージパケット識別子の1以上の対が抽出された場合、所定の規定に従って前記抽出された対の少なくとも1つを自動的に識別す

ること

を含み、

前記受信した複数の対のそれぞれが、条件付きアクセス資格制御メッセージ識別子（C A E C M）またはローカル資格制御メッセージ識別子（L E C M）のどちらかを含む

ことを特徴とする方法。

【請求項5】 所定の規定が、前記対が抽出された順番によって異なることを特徴とする請求項4に記載の方法。

【請求項6】 前記受信した対のそれぞれが、サービス識別子をさらに含むことを特徴とする請求項4に記載の方法。

【請求項7】 前記所定の規定が、受信されるべき対の第1の対をサービス識別子およびローカル資格制御メッセージ識別子を含むと定義することを特徴とする請求項4に記載の方法。

【請求項8】 前記データの少なくとも一部が、複数の条件付きアクセスシステムのうちの1つを用いてセキュリティ保護されることを特徴とする請求項4に記載の方法。

【請求項9】 前記条件付きアクセスシステムのうちの少なくとも1つが、前記プログラムの放送業者に関連付けられており、少なくとも第2の条件付きアクセスシステムがアクセスデバイスに関連付けられており、前記表示デバイスと通信可能であることを特徴とする請求項8に記載の方法。

【請求項10】 前記表示デバイスがデジタルテレビジョンであり、前記アクセスデバイスが第2のセキュリティデバイスと組み合わされたセットトップボックスであることを特徴とする請求項9に記載の方法。

【請求項11】 セキュリティデバイスが、インターフェース保護関連情報と条件付きアクセス関連情報とをオーディオ／ビデオ処理デバイスに伝達すること、および

オーディオ／ビデオ処理デバイスが、前記伝達された条件付きアクセス情報と記憶されている条件付きアクセス情報とを用いてプログラムマップテーブルを分解することを含み、

前記プログラムマップテーブルがパケット識別子を対応するサービス情報に関連付けることを特徴とする請求項4に記載の方法。

【請求項12】 前記プログラムを示すデータをスクランブル解除するのに適した資格制御メッセージデータをどのパケットが含んでいるかを識別するように、前記セキュリティデバイスが、パケット識別子を使用することを特徴とする請求項11に記載の方法。

【請求項13】 前記資格制御メッセージの少なくともいくつかは、少なくとも、識別およびL E C M用フィールドと、条件付きアクセス識別用フィールドとを含むローカル資格制御メッセージであり、前記正当な処理が、前記識別およびL E C M用フィールドと前記条件付きアクセス識別用フィールドのうちの少なくとも1つに含まれる情報を用いて前記データの適切な鍵にアクセスすることによって前記サービスをスクランブル解除することを含むことを特徴とする請求項12に記載の方法。

【請求項14】 前記データの少なくとも1つの部分が少なくとも1つのプログラムを示すことを特徴とする請求項8に記載の方法。

【請求項15】 前記データがデジタル伝送システムを介して伝達されることを特徴とする請求項4に記載の方法。

【請求項16】 放送業者資格制御メッセージからローカル資格制御メッセージを識別するための方法であって、

サービスおよび資格制御メッセージパケット識別子の対を、サービスに関連付けられたデータから抽出するステップと、

サービスおよび資格制御メッセージパケット識別子の対が1つだけ抽出された場合、前記抽出された対がローカル資格制御メッセージまたは放送資格制御メッセージのどちらかであることを確認するステップと、

サービスおよび資格制御メッセージパケット識別子の1以上の対が抽出された場合、前記抽出された対の少なくとも1つがローカル資格制御メッセージであることを自動的に確認するステップと

を含むことを特徴とする方法。

【請求項17】 放送資格制御メッセージからローカル資格制御メッセージ

を識別するための方法であって、

サービスに関連付けられたデータからサービスおよび資格制御メッセージパケット識別子の対を抽出するステップと、

サービスおよび資格制御メッセージパケット識別子の対が1つだけ抽出された場合、前記抽出された対がローカル資格制御メッセージまたは放送資格制御メッセージのどちらかであることを確認するステップと、

サービスおよび資格制御メッセージパケット識別子の1以上の対が抽出された場合、前記抽出された対の少なくとも1つが放送資格制御メッセージであることを自動的に確認するステップと

を含むことを特徴とする方法。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0004

【補正方法】変更

【補正の内容】

【0004】

サイマルクリプトベースのCAシステムでは、デジタルテレビジョン(DTV)等のデジタルオーディオ/ビデオ処理システムは、PMTを分解し、CAモジュールから獲得したCAシステム識別(ID)を用いてサービスおよびECMPIDを抽出する。通常、各CAモジュールは、1つのCAシステムだけをサポートし、したがって1つのCAシステムIDだけを有する。A/VパケットのPIDと制御ワード(CW)を伝えるECMのPIDとが、正規の購入資格を有するプログラムをスクランブル解除するCAモジュールに送信される。

Wasilewskiによる米国特許第5,420,866号は、サイマルクリプトシステムに酷似した複数の異なるデコーダに対して条件付きアクセス情報を提供するための方法を記載している。Wasilewskiは、異なるCAプロバイダを識別するためにCAシステム識別パラメータCA_____System_____ID、したがって異なるデコーダを使用することを述べている(列12、行12-16参照のこと)。

また、Daniel Kramerによる「Wunderkiste des digitalen Fernsehens」という名称の記事は、サイマルクリプト技術について記述している（Kramer D:「Wunderkiste des digitalen Fernsehens」Bull. SEV/VSE, CH, Schweizerischer Elektrotechnischer Verein, Zurich, Vol. 88, No. 3, pp. 27-30）。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int. Patent Application No.
PCT/US 00/27685

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04N7/16 H04N5/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-internal, COMPENDEX, INSPEC, IBM-TDS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 420 865 A (WASILEWSKI ANTHONY J) 30 May 1995 (1995-05-30) column 1, line 14 -column 7, line 7 figures 1-8	1, 4, 9 2, 3, 5-8, 10-16
A	WO 00 56068 A (THOMSON LICENSING S A ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET) 21 September 2000 (2000-09-21) page 2, line 14 - line 29 page 4, line 4 -page 5, line 14 figures 1-8	1, 3
P, X	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) column 1, line 12 -column 7, line 20 figures 1-5	1-16
A	---	---
	--- -/--	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is used to establish the publication date of another citation or other special reason (as specified) "U" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is considered with one or more other such documents, such combination being obvious to a person skilled in the art. "Z" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
30 January 2001		06/02/2001
Name and mailing address of the ISA European Patent Office, P.O. Box 5011 Patentstr. 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040 Tx. 31 651 apo nl Fax (+31-70) 340-2016		Authorized officer Tito Martins, J

Form PCT/ISA/210 (patent search) (July 1999)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/27685

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM", EBU REVIEW-TECHNICAL, BE, EUROPEAN BROADCASTING UNION, BRUSSELS, NR. 266, PAGE(S) 64-77 XPO00559450 ISSN: 0251-0936 the whole document</p>	1-16
A	<p>KRAMER D: "WUNDERKISTE DES DIGITALEN FERNSEHENS", BULLETIN SEV/VSE, CH, SCHWEIZERISCHER ELEKTROTECHNISCHER VEREIN, ZURICH, VOL. 88, NR. 3, PAGE(S) 27-30 XPO00886105 ISSN: 0036-1321 page 27-28</p>	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/US 00/27685

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5420866 A	30-05-1995	AU 687844 B	05-03-1998
		AU 7220994 A	17-10-1995
		CA 2186368 A,C	05-10-1995
		JP 2940639 B	25-08-1999
		JP 9511369 T	11-11-1997
		WO 9526597 A	05-10-1995
WO 0056068 A	21-09-2000	AU 3629109 A	04-10-2000
EP 0858184 A	12-08-1998	IL 120174 A	28-10-1999
		GB 2322030 A,B	12-08-1998

 フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(72)発明者 マイケル スコット デイス
アメリカ合衆国 46077 インディアナ州
ジョーンズビル インディアン パイプ
レーン 1103

(72)発明者 ジャンールイ ディアスコーン
アメリカ合衆国 46032 インディアナ州
カーメル アーバー ドライブ 496

(72)発明者 デイビッド ジェイ ダフィールド
アメリカ合衆国 46220 インディアナ州
インディアナポリス フォール クリー
ク ロード 5459

Fターム(参考) 5C064 BA07 BB02 BC06 BC17 BC18
BC22 BC23 BD02 BD08 BD09
CA14 CB01 CC01 CC04
5J104 AA12 EA04 KA02 NA01 PA05